ABSTRACT

A digital wallet stores an cryptographically camouflaged access-controlled datum, e.g., a private key encrypted under the user's PIN. Entry of the correct PIN will correctly decrypt the stored key. Entry of certain pseudo-valid PINs will also decrypt the stored key, but improperly so, resulting in a candidate key indistinguishable from the correct key. Such pseudo-valid PINs are spread thinly over the space of PINs, so that the user is unlikely to realize a pseudo-valid PIN via a typographical error in entering the correct PIN. In existing wallet technologies, which lack pseudo-valid PINs, only the correct PIN produces a decrypted key; thus, hackers can find the correct PIN by entering all possible PINs until a key is produced. The present invention's plurality of candidate keys prevent a hacker from knowing when he has found the correct key. In addition, hacker detection may be moved off-line into devices accepting messages signed with candidate keys, and/or the lockout threshold may be increased. Thus, the wallet can be forgiving of typographic or transposition errors, yet a hacker trying large numbers of PINs will eventually guess a pseudo-valid (but still incorrect) PIN and recover a candidate private key whose fraudulent use will be detected. The wallet may be used with associated key generation, certification, and verification technologies. Such technologies may include pseudo-public keys embedded in pseudo-public certificates, i.e., public keys that are not generally known and which are contained in certificates that are verifiable only by entities so authorized by the certifying authority.